# IME を使用した IPS TCP リセット設定

## 目次


概要
前提条件
要件
使用するコンポーネント
表記法
設定
ネットワーク図
設定
センサー設定を開始して下さい
IME にセンサーを追加して下さい
Cisco IOS ルータのための TCP Reset を設定して下さい
確認
攻撃および TCP Reset を起動させて下さい
トラブルシューティング
ヒント
関連情報


## 概要

この資料は IPS Manager Express （IME）を使用して侵入防御システム（IPS） TCP Reset の設定を説明します。 IME および IPS センサーが TCP Reset のための Ciscoルータを管理するのに使用されています。 この設定を検討するとき、これらの項目を覚えて下さい:

- センサーをインストールし、センサー作業をきちんと確かめて下さい。
- スニフィング インターフェイスのスパンを、インターフェイス外部のルータまで及ぶようにします。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IPS Manager Express 7.0

- Cisco IPS センサー 7.0(0.88)E3
- Cisco IOS ソフトウェア リリース 12.4 の Cisco IOS® ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 設定

## ネットワーク図

このドキュメントでは、次の図で示されるネットワーク構成を使用しています。

## 設定

このドキュメントでは、次に示す設定を使用しています。

- Router Light
- Router House

**Router Light**

```
Current configuration : 906 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname light ! enable password cisco ! username cisco
password 0 cisco ip subnet-zero ! ! ! ip ssh time-out
120 ip ssh authentication-retries 3 ! call rsvp-sync ! !
! fax interface-type modem mta receive maximum-
recipients 0 ! controller E1 2/0 ! ! ! interface
FastEthernet0/0 ip address 10.100.100.2 255.255.255.0
duplex auto speed auto ! interface FastEthernet0/1 ip
address 1.1.1.1 255.255.255.0 duplex auto speed auto !
interface BRI4/0 no ip address shutdown ! interface
BRI4/1 no ip address shutdown ! interface BRI4/2 no ip
address shutdown ! interface BRI4/3 no ip address
shutdown ! ip classless ip route 0.0.0.0 0.0.0.0
10.100.100.1 ip http server ip pim bidir-enable ! !
dial-peer cor custom ! ! line con 0 line 97 108 line aux
0 line vty 0 4 login ! end
```

**Router House**

```
Current configuration : 939 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname house ! logging queue-limit 100 enable password
cisco ! ip subnet-zero ! ! no ip cef no ip domain lookup
! ip audit notify log ip audit po max-events 100 ! ! no
voice hpi capture buffer no voice hpi capture
destination ! ! ! ! interface FastEthernet0/0 ip address
10.66.79.210 255.255.255.224 duplex auto speed auto !
interface FastEthernet0/1 ip address 10.100.100.1
255.255.255.0 duplex auto speed auto ! interface ATM1/0
no ip address shutdown no atm ilmi-keepalive ! ip
classless ip route 0.0.0.0 0.0.0.0 10.66.79.193 ip route
1.1.1.0 255.255.255.0 10.100.100.2 no ip http server no
ip http secure-server ! ! ! ! call rsvp-sync ! ! mgcp
profile default ! ! line con 0 exec-timeout 0 0 line aux
0 line vty 0 4 exec-timeout 0 0 password cisco login
line vty 5 15 login ! ! end
```

## センサー設定を開始して下さい

センサーの設定を開始するためにこれらのステップを完了して下さい。

1. これがセンサーにログイン する 初めてである場合ユーザネームとして cisco およびパスワードとして cisco を入力して下さい。
2. システムがパスワード変更のプロンプトを表示したら、パスワードを変更します。**注**：Cisco123 は辞書ワードで、システムで許されません。
3. **セットアップを**入力し、センサーのための基本的なパラメータを設定するためにシステムプロンプトを完了して下さい。
4. 次の情報を入力します。
```
sensor5#setup --- System Configuration Dialog --- !--- At any point
you may enter a question mark '?' for help. !--- Use ctrl-c to abort the configuration
dialog at any prompt. !--- Default settings are in square brackets '[]'. Current
Configuration: networkParams ipAddress 10.66.79.195 netmask 255.255.255.224 defaultGateway
10.66.79.193 hostname Corp-IPS telnetOption enabled !--- Permit the IP address of
workstation or network with IME accessList ipAddress 10.66.79.0 netmask 255.255.255.0 exit
timeParams summerTimeParams active-selection none exit exit service webServer general ports
443 exit exit
```
5. 設定を保存します。センサーが設定を保存することができるように数分かかる場合があります。
```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
```

## IME にセンサーを追加して下さい

IME にセンサーを追加するためにこれらのステップを完了して下さい:

1. IPS Manager Express をインストールした、行き IPS Manager Express を開いて下さい Windows PC に。
2. **> Add を**『Home』 を選択 して下さい。
3. この情報を入力し、設定を終了するために『OK』 をクリック して下さい。
4. **> Corp IPS** センサー ステータスを確認し、次に『Device Status』 を選択 するために右クリックするために『Devices』 を選択 して下さい。表示できることを確かめて下さい

# Cisco IOS ルータのための TCP Reset を設定して下さい

Cisco IOS ルータのための TCP Reset を設定するためにこれらのステップを完了して下さい:

1. IME PC から、Webブラウザを開き、**https://10.66.79.195** に行って下さい。
2. センサーからダウンロードされる HTTPS 認証を受け入れるために『OK』 をクリック して下さい。
3. Login ウィンドウで、ユーザ名に cisco、パスワードに 123cisco123 を入力します。この IME マネージメントインターフェイスは現われます:
4. Configuration タブから、**アクティブなシグニチャを**クリックして下さい。
5. それから『Signature Wizard』 をクリック して下さい。
6. ウィザードで、シグニチャ エンジンとして**ストリング TCP を**『Yes』 を選択 し、選択して下さい。 [Next] をクリックします。
7. efdault としてこの情報を残すか、またはあなた自身のシグニチャ ID、シグニチャ名前およびユーザ メモを入力することができます。 [Next] をクリックします。
8. **検知時のアクションを**選択し、**生成 します アラート**および**リセット TCP 接続を**選択して下さい。 それから**次に**続くために『OK』 をクリック すれば。
9. 正規表現を入力すれば、`testattack` この例で使用されます。 サービス ポートのための **23 を**入力し、方向のために**保守することを**選択し続くために『Next』 をクリック して下さい。
10. デフォルトとしてこの情報を残すことができます。 [Next] をクリックします。
11. ウィザードを終えるために『Finish』 をクリック して下さい。
12. **> sig0 > アクティブなシグニチャ**新しく作成されたシグニチャを **SIG ID** か **SIG 名前**によって見つけるために『Configuration』 を選択 して下さい。 シグニチャを表示するために『Edit』 をクリック して下さい。
13. センサーにシグニチャを加えるために **Apply ボタンを**確認した、クリックする後『OK』 をクリック して下さい。

## 確認

### 攻撃および TCP Reset を起動させて下さい

攻撃および TCP Reset を起動させるためにこれらのステップを完了して下さい:

1. 攻撃を開始する前に、行き、**イベントモニタリングを > 廃棄された不正侵入ビューは IME** に選択し、右のセンサーを選択します。
2. Router Light から Router House に Telnet 接続し、testattack と入力します。Telnetセッションを再設定するために **<space> か <enter> を**見つけて下さい。
```
light#telnet 10.100.100.1
Trying 10.100.100.1 ... Open User Access Verification Password: house>en Password:
house#testattack [Connection to 10.100.100.1 closed by foreign host] !--- Telnet session
has been reset due to the !--- signature "String.tcp" triggered.
```
3. IPS イベント ビューアのダッシュボードから、赤い警告灯は攻撃が開始すれば現われます。

## トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

### ヒント

これらのトラブルシューティング に 役立つ ヒントを使用して下さい:

- コマンドおよびコントロール ポートからシャニング（排除機能）を実行すると、ルータの access control list（ACL; アクセス コントロール リスト）が再プログラムされます。 TCP Reset は、Sensor のスニフィング インターフェイスから送信されます。 ここに示されているように有効に なる両方の着信パケットによってスイッチの **set span**、**set span <src_mod/src_port><dest_mod/dest_port>** コマンドを使用する時。`banana (enable)`**`set span 2/12 3/6 both inpkts enable Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/12 Incoming Packets enabled. Learning enabled. Multicast enabled.`** `banana (enable) banana (enable) banana (enable)`**`show span`** `Destination : Port 3/6 !--- connect to sniffing interface of the sensor Admin Source : Port 2/12 !--- connect to FastEthernet0/0 of Router House Oper Source : Port 2/12 Direction : transmit/receive Incoming Packets: enabled Multicast : enabled`
- TCP Reset が動作している場合は、アクション タイプ TCP Reset に対してアラームがトリガされるかどうかを確認してください。 アラームが現われる場合、シグニチャ型が TCP Reset に設定 されることを確認して下さい。このコマンドを定着させ、発行するためにサービス アカウント SU を使用してログインして下さい。 このコマンドは検知インターフェイスが eth0 に設定 されることを仮定します。`[root@sensor1 root]#`**`tcpdump -i eth0 -n`** **注:** 百の TCP リセットは対象/ターゲットそれから百に送信 されて得ます攻撃者/クライアントに送信されて得ます。次に出力例を示します。

```
03:06:00.598777 64.104.209.205.1409 >
 10.66.79.38.telnet: R 107:107(0) ack 72 win 0
03:06:00.598794 64.104.209.205.1409 >
 10.66.79.38.telnet: R 108:108(0) ack 72 win 0

03:06:00.599360 10.66.79.38.telnet >
 64.104.209.205.1409: R 72:72(0) ack 46 win 0
03:06:00.599377 10.66.79.38.telnet >
 64.104.209.205.1409: R 73:73(0) ack 46 win 0
```

## 関連情報

- Cisco Secure Intrusion Prevention のサポート ページ
- Cisco Secure Intrusion Prevention System のためのシスコのドキュメント
- テクニカルサポートとドキュメント - Cisco Systems